SOLUTION BRIEF

Achieving PCI DSS Compliance with Lacework

OVERVIEW

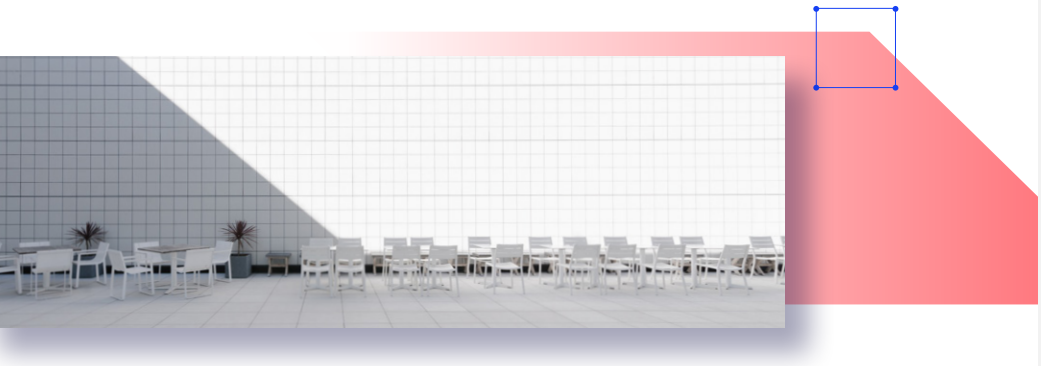
An industry standard

The Payment Card Industry Data Security Standard (PCI DSS) is a set of compliance requirements that helps organizations maintain security while processing, storing, and transmitting sensitive credit card information. Managed by the PCI Security Standards Council (PCI SSC), PCI DSS requires payment brands and acquirers to enforce compliance. By providing standards and materials like specification frameworks, the PCI SSC enables businesses to maintain data security when it comes to managing servers and accounts that store or process credit card data. Achieving PCI DSS compliance is important for confirming the security of your systems, as well as winning the trust of customers and payment brands.

CHALLENGES

Proving PCI compliance

The most difficult part of achieving PCI is having to prove compliance with the framework. Since it's meant to be flexible enough to allow companies leeway on how they meet the guidelines, it's necessary to gather a lot of evidence both before and during the audit. If your organization has never achieved PCI before, you also face the unknown cost and risk of preparing for an audit and potentially going through a pre-audit to make sure the final audit is successful. PCI pre-audits and audits, along with the accompanying need to gather evidence, are time-consuming and expensive.



Key Lacework use cases

- Asset management to track cloud resources
- Automated monitoring throughout development lifecycle
- Continuous vulnerability scanning integrated with alert channels
- Dashboard that visualizes compliance posture
- One-click reporting

OUR APPROACH

Visibility and speed

Lacework can help with PCI audits by easily providing a comprehensive view of your cloud environment and mapping PCI controls to the required cloud security controls. Lacework reports can be run at any point in time to review compliance against your multicloud and multi-account environment, allowing your compliance team and cloud team to work together to ensure continued compliance to PCI. Additionally, Lacework reports can be run and reviewed over different time periods, so any compliance drifts can be reviewed and investigated. Lacework also facilitates the auditing process: at any time, you can choose to run a report that shows exactly how your cloud environment implements PCI controls, which you can then provide to an auditor. The Polygraph® Data Platform saves you time and money by preventing issues before the audit and by reducing the evidence gathering time during the audit.

Lacework acts as a "flight recorder" for your environment, collecting and organizing PCI-relevant data. We enable organizations to easily meet auditors' evidence gathering requests, drastically reducing the amount of time required for the security team. In addition, we track this data over time so that you can always go back and review changes to ensure better control of their audited environment.

The Polygraph® Data Platform saves you time and money by preventing issues before the audit and by reducing the evidence gathering time during the audit.

USE CASES

The Lacework advantage

The Lacework platform contains many features that will help streamline your journey to PCI compliance, including:

Asset management

Track your cloud resources with the Lacework resource management function. You can edit the resources summary to show different information, including Resource Name, Account ID, Account Alias, Service, Type, Status, etc. You can also export the resource summary to a CSV file, which you can use as evidence of your organization's cloud asset inventory.

Logging and monitoring

Automated monitoring and reporting throughout the development lifecycle helps ensure that you're compliant from day one. Lacework monitors all events, configurations, and behavioral activities on the cloud, offering you a complete view of your entire cloud ecosystem. The events dashboard gives an overview of all events that have been logged in their environment. Event records include a description of why the event was triggered, which account was responsible, what API was affected, and the source IP address. Lacework also enables you to send high fidelity contextual alerts to your SIEM solution.

Vulnerability scanning

By managing vulnerabilities and compliance continuously, you can mitigate risk as it is introduced into your cloud infrastructure. Lacework automatically and continuously scans your organization's cloud environment for vulnerabilities, which we communicate via alert channels configured by the admin user. The Lacework Vulnerability Assessment summary shows a list of all identified vulnerabilities and rates them based on criticality. You can then export the report to a CSV file to share with auditors.

Lacework monitors all events, configurations, and behavioral activities on the cloud, offering you a complete view of your entire cloud ecosystem.

Host intrusion detection system (HIDS)

Lacework acts as a host-based intrusion detection system (HIDS) where an agent is loaded into various types of Linux workloads to gain visibility into changes in baseline behaviors. Lacework can also monitor Kubernetes-based workloads as well as files within containers and VMs.

File Integrity Monitoring (FIM)

Lacework can monitor the most sensitive files on your workloads. Our agent includes file integrity monitoring (FIM), which is used to ensure important files on the operating system are not modified in an unintended or malicious way. When a monitored file is changed, an alert will be generated in Lacework and sent to the appropriate teams for remediation.

Compliance over time

Lacework allows for tracking of compliance standards over time. A user can run a compliance report at any time to see the compliance status on an hour-by-hour basis. This enables tracking of compliance status to see what has changed and who changed it.

Communication and information

The Lacework compliance dashboard provides an overview of your organization's compliance posture across several accounts. It also groups the PCI technical controls into a readable PDF or CSV format. The report covers areas such as identity and access management, logging and monitoring, networking, and general security. Plus, it displays how your organization's cloud configurations are mapped to specific PCI criteria, showing which need to be addressed and fixed. With our one-click reporting, you can stop aggregating reports from multiple systems, and start responding to auditors instantly.

AT A GLANCE

Lacework helps businesses achieve PCI DSS compliance by offering:

- Compliance reporting and configuration assurance
- Cloud user and entity behavior analytics (UEBA)
- Container and Kubernetes security (HIDS and vulnerability detection)
- Intrusion detection (for hosts, containers, and Kubernetes)
- File integrity monitoring (for hosts, containers, and Kubernetes)
- Anti-malware (for hosts, containers, and Kubernetes)
- Vulnerability scanning (for hosts and containers)

Mapping required security controls

PCI Compliance Requirements Solved with Lacework	PCI Requirements	Lacework Platform Support
Continuous Monitoring	**Requirement 1:** Install and maintain a firewall and router configuration to protect cardholder data (1.5) **Requirement 6:** Develop and maintain secure systems and applications (6.3, 6.5, 6.6) **Requirement 10:** Track and monitor all access to network resources and cardholder data (10.6) **Requirement 11:** Regularly test security systems and processes (11.4, 11.5) **Requirement 12:** Maintain a policy that addresses information security for all personnel (12.10)	Included
Alerting	**Requirement 6:** Develop and maintain secure systems and applications (6.1, 6.2, 6.4, 6.5, 6.7) **Requirement 7:** Restrict access to cardholder data by business need to know (7.2, 7.3) **Requirement 8:** Assign a unique ID to each person with computer access (8.1, 8.7) **Requirement 11:** Regularly test security systems and processes (11.2, 11.5, 11.6)	Included
Detecting, Investigating, and Verifying	**Requirement 10:** Track and monitor all access to network resources and cardholder data (10.1, 10.2, 10.3, 10.5, 10.6, 10.7, 10.8) **Requirement A1** (1.3, 1.4)	Included
Maintaining and Continuously Evaluating Systems	**Requirement 12:** Maintain a policy that addresses information security for all personnel (12.2, 12.5, 12.10)	Included

Ready to chat?

Request a demo

Are you an existing customer? You can now find Lacework in the Google Cloud Marketplace!